19.5 DNS, DHCP, Gateway und NAT Spickzettel

Dieser Spickzettel fasst vier sehr häufige Prüfungsthemen zusammen:

- DNS
- DHCP
- Gateway
- NAT

Diese Begriffe werden in Aufgaben oft gemeinsam geprüft, weil sie für normalen Netzwerkzugriff zusammenwirken.

Merksatz:

DNS findet Namen.
DHCP verteilt Konfiguration.
Gateway führt in andere Netze.
NAT übersetzt Adressen.

Grundidee im Überblick

Begriff	Hauptaufgabe	Typisches Fehlerbild
DNS	Namen in IP-Adressen auflösen	IP geht, Name nicht
DHCP	IP-Konfiguration automatisch verteilen	169.254.x.x oder falsche IP
Gateway	Weg in andere Netze bereitstellen	lokal geht, Internet nicht
NAT	private Adressen in öffentliche Adressen übersetzen	intern geht, extern nicht oder Portweiterleitung fehlerhaft

Merksatz:

Jeder Begriff löst ein anderes Problem.

DNS kurz erklärt

DNS steht für:

Domain Name System

Aufgabe:

```
DNS übersetzt Namen in IP-Adressen.
```

Beispiel:

```
www.example.com
```

wird aufgelöst zu:

```
einer IPv4- oder IPv6-Adresse
```

Merksatz:

```
DNS ist das Namenssystem des Netzwerks.
```

DNS-Frage in der Prüfung

Typisches Fehlerbild:

```
Webseite ist per IP-Adresse erreichbar,
aber nicht per Domainname.
```

Wahrscheinliche Ursache:

```
DNS-Problem
```

Mögliche Ursachen:

```
falscher DNS-Server
DNS-Server nicht erreichbar
falscher DNS-Eintrag
DNS-Cache veraltet
DNS-Suffix falsch
Split-DNS bei VPN falsch
Firewall blockiert DNS
```

Merksatz:

```
IP ja,
Name nein:
DNS prüfen.
```

Wichtige DNS-Records

Record	Bedeutung
A	Name zu IPv4-Adresse
AAAA	Name zu IPv6-Adresse
CNAME	Alias auf anderen Namen
MX	Mailserver einer Domain
TXT	Textinformationen, zum Beispiel SPF
NS	zuständiger Nameserver
PTR	Reverse DNS, IP-Adresse zu Name

Merksatz:

```
A ist IPv4.
AAAA ist IPv6.
MX ist Mail.
PTR ist rückwärts.
```

DNS und Ports

DNS nutzt:

```
UDP 53

und bei Bedarf

TCP 53
```

UDP 53:

normale DNS-Abfragen

TCP 53:

große Antworten,
Zonentransfers
oder bestimmte Spezialfälle

Merksatz:

DNS ist meistens UDP 53,
aber TCP 53 nicht vergessen.

DNS-Prüfung mit Werkzeugen

Typische Werkzeuge:

nslookup

dig

ping mit Namen

Browser-Test

DNS-Cache prüfen

Wichtig:

ping auf Name testet DNS und ICMP zusammen.

Besser für reine DNS-Prüfung:

nslookup

oder

```
dig
```

Merksatz:

```
DNS gezielt mit nslookup oder dig prüfen.
```

DNS-Cache

Ein DNS-Cache speichert bereits aufgelöste Namen.

Vorteile:

```
schnellere Namensauflösung
weniger DNS-Anfragen
```

Problem:

```
veraltete Einträge können Fehler verursachen.
```

Merksatz:

```
DNS-Cache kann alte Informationen enthalten.
```

DNS-Suffix

Ein DNS-Suffix ergänzt unvollständige Namen.

Beispiel:

```
server01
```

kann ergänzt werden zu:

```
server01.firma.local
```

Typische Fehler:

```
falsches Suchsuffix
anderes Suffix im VPN
interner Name wird extern nicht gefunden
```

Merksatz:

```
DNS-Suffix hilft bei kurzen internen Namen.
```

Split-DNS

Split-DNS bedeutet:

```
interne und externe DNS-Auflösung können unterschiedliche Antworten liefern.
```

Beispiel:

```
intern:
intranet.firma.de zeigt auf private IP-Adresse

extern:
intranet.firma.de ist nicht erreichbar
oder zeigt auf öffentliche Adresse
```

Typisch bei:

```
VPN
Intranet
internen Diensten
Hybrid-Umgebungen
```

Merksatz:

```
Split-DNS kann je nach Standort unterschiedliche IPs liefern.
```

DHCP kurz erklärt

DHCP steht für:

Dynamic Host Configuration Protocol

Aufgabe:

DHCP verteilt automatisch Netzwerkkonfiguration an Clients.

Typische Informationen:

IP-Adresse
Subnetzmaske
Standardgateway
DNS-Server
Lease-Zeit
weitere Optionen

Merksatz:

DHCP erspart manuelle IP-Konfiguration.

DHCP-DORA

DORA beschreibt den DHCP-Ablauf:

Schritt	Bedeutung
Discover	Client sucht DHCP-Server
Offer	Server bietet Konfiguration an
Request	Client fordert angebotene Konfiguration an
Acknowledge	Server bestätigt die Vergabe

Merksatz:

DHCP-DORA:
Discover,
Offer,
Request,
Acknowledge.

DHCP und Ports

DHCP nutzt:

Rolle	Protokoll	Port
DHCP-Server	UDP	67
DHCP-Client	UDP	68

Merksatz:

```
DHCP nutzt UDP 67 und UDP 68.
```

DHCP und Broadcast

Ein Client hat zu Beginn oft noch keine gültige IP-Adresse.

Deshalb nutzt DHCP am Anfang Broadcast.

Grund:

```
Der Client kennt den DHCP-Server noch nicht.
Der Client hat noch keine vollständige Netzwerkkonfiguration.
```

Merksatz:

```
DHCP beginnt häufig mit Broadcast.
```

APIPA

APIPA steht für:

```
Automatic Private IP Addressing
```

Bereich:

```
169.254.0.0/16
```

Bedeutung:

```
Der Client hat keine gültige DHCP-Adresse erhalten
und vergibt sich selbst eine automatische Adresse.
```

Typisches Fehlerbild:

```
Client hat 169.254.x.x
und erreicht keine normalen Netzressourcen.
```

Merksatz:

```
169.254.x.x deutet auf DHCP-Problem hin.
```

DHCP-Scope

Ein DHCP-Scope ist ein Adressbereich, aus dem DHCP Adressen vergeben darf.

Beispiel:

```
192.168.10.100 bis 192.168.10.200
```

Zu einem Scope gehören oft:

```
IP-Bereich
Subnetzmaske
Gateway
DNS-Server
Lease-Zeit
Ausschlüsse
Reservierungen
```

Merksatz:

```
DHCP-Scope = Adresspool für automatische Vergabe.
```

DHCP-Lease

Eine Lease ist die zeitlich begrenzte Vergabe einer IP-Adresse.

Bedeutung:

```
Ein Client erhält eine Adresse nicht für immer,
sondern für eine bestimmte Lease-Zeit.
```

Vorteil:

```
Adressen können später wiederverwendet werden.
```

Merksatz:

```
DHCP-Lease = zeitlich begrenzte IP-Vergabe.
```

DHCP-Reservierung

Eine DHCP-Reservierung weist einem bestimmten Gerät immer dieselbe IP-Adresse zu.

Meist anhand der:

```
MAC-Adresse
```

Typisch für:

```
Drucker
Server
NAS
Netzwerkgeräte
wichtige Clients
```

Merksatz:

```
Reservierung bedeutet:
automatisch,
aber immer dieselbe Adresse.
```

DHCP-Relay

Ein DHCP-Relay leitet DHCP-Anfragen in ein anderes Netz weiter.

Warum nötig?

> DHCP-Broadcasts werden normalerweise nicht über Router weitergeleitet.

Beispiel:

> Client in VLAN 20
>
> DHCP-Server in VLAN 10

Dann braucht man oft:

> DHCP-Relay

Merksatz:

> DHCP-Relay hilft,
> wenn Client und DHCP-Server in unterschiedlichen Netzen sind.

DHCP-Fehlerbilder

Fehlerbild	Mögliche Ursache
169.254.x.x	DHCP nicht erreicht
falsches Gateway	falsche DHCP-Option
falscher DNS-Server	falsche DHCP-Option
keine Adresse mehr frei	Scope erschöpft
nur ein VLAN betroffen	DHCP-Relay oder VLAN falsch
manche Geräte bekommen falsche IP	falscher Scope oder falsches VLAN
Gerät bekommt alte IP	Lease oder Reservierung prüfen

Merksatz:

> DHCP-Probleme betreffen IP-Konfiguration,
> nicht Namensauflösung.

Gateway kurz erklärt

Das Standardgateway ist der Router, über den ein Host andere Netze erreicht.

Ohne Gateway kann ein Host normalerweise nur mit Geräten im eigenen Subnetz kommunizieren.

Beispiel:

```
Client:
192.168.10.50/24

Gateway:
192.168.10.1
```

Merksatz:

```
Gateway = Ausgang in andere Netze.
```

Gateway muss im lokalen Netz liegen

Das Gateway muss für den Client lokal erreichbar sein.

Falsches Beispiel:

```
Client:
192.168.10.50/24

Gateway:
192.168.20.1
```

Problem:

```
Client liegt im Netz 192.168.10.0/24.
Gateway liegt im Netz 192.168.20.0/24.
```

Der Client erreicht sein Gateway nicht lokal.

Merksatz:

Standardgateway muss im gleichen lokalen Subnetz erreichbar sein.

Gateway-Fehler in der Prüfung

Typisches Fehlerbild:

Client erreicht lokale Geräte,
aber keine externen Netze.

Wahrscheinliche Ursache:

Gateway fehlt
oder Gateway falsch

Auch möglich:

Routingfehler
NAT-Problem
Firewall blockiert
Providerverbindung gestört

Merksatz:

Lokal ja,
extern nein:
Gateway,
Routing,
NAT
oder Firewall prüfen.

Routing kurz erklärt

Routing bedeutet:

Weiterleitung von Paketen zwischen verschiedenen IP-Netzen.

Ein Router entscheidet anhand seiner Routing-Tabelle, wohin ein Paket weitergeleitet wird.

Routing-Tabelle enthält typischerweise:

```
Zielnetz
Next Hop
Interface
Metrik
```

Merksatz:

```
Routing verbindet Netze.
```

Standardroute

Eine Standardroute ist die Route für alle Ziele, für die keine speziellere Route existiert.

Schreibweise IPv4:

```
0.0.0.0/0
```

Merksatz:

```
Standardroute = Weg für unbekannte Ziele.
```

Spezifischste Route gewinnt

Wenn mehrere Routen passen, wird die spezifischste Route verwendet.

Beispiel:

```
192.168.10.0/24
```

ist spezifischer als:

```
192.168.0.0/16
```

Merksatz:

Längster passender Präfix gewinnt.

NAT kurz erklärt

NAT steht für:

Network Address Translation

Aufgabe:

NAT übersetzt IP-Adressen.

Häufiger Einsatz:

private interne IPv4-Adressen werden beim Zugriff ins Internet
in eine öffentliche IPv4-Adresse übersetzt.

Merksatz:

NAT übersetzt Adressen.

Warum NAT verwendet wird

Gründe:

private IPv4-Adressen im LAN nutzen
öffentliche IPv4-Adressen sparen
interne Adressen nach außen verbergen
Internetzugriff für viele Clients ermöglichen

Wichtig:

NAT ist keine vollständige Sicherheitsmaßnahme.

Merksatz:

NAT hilft bei Adressübersetzung,
ersetzt aber keine Firewall.

Private IPv4-Bereiche

Bereich	CIDR
10.0.0.0 bis 10.255.255.255	10.0.0.0/8
172.16.0.0 bis 172.31.255.255	172.16.0.0/12
192.168.0.0 bis 192.168.255.255	192.168.0.0/16

Merksatz:

Private IPv4-Adressen werden im Internet nicht direkt geroutet.

PAT kurz erklärt

PAT steht für:

Port Address Translation

PAT ist eine Form von NAT, bei der zusätzlich Portnummern zur Zuordnung genutzt werden.

Zweck:

viele interne Clients können über eine öffentliche IP-Adresse ins Internet.

Merksatz:

PAT nutzt Ports zur Unterscheidung mehrerer Verbindungen.

NAT und PAT vergleichen

Begriff	Bedeutung	Typischer Einsatz
NAT	übersetzt IP-Adressen	private zu öffentliche IP
PAT	übersetzt IP-Adressen und Ports	viele Clients über eine öffentliche IP

Begriff	Bedeutung	Typischer Einsatz
Portweiterleitung	leitet externen Port intern weiter	internen Dienst von außen erreichbar machen

Merksatz:

```
NAT übersetzt Adressen.
PAT unterscheidet Verbindungen über Ports.
```

Portweiterleitung kurz erklärt

Portweiterleitung bedeutet:

```
eingehender Verkehr auf einem externen Port
wird an einen internen Dienst weitergeleitet.
```

Beispiel:

```
öffentliche IP: TCP 443

wird weitergeleitet an:

interner Webserver: TCP 443
```

Merksatz:

```
Portweiterleitung macht interne Dienste von außen erreichbar.
```

Portweiterleitung und Risiko

Portweiterleitung erhöht die Angriffsfläche, weil ein interner Dienst von außen erreichbar wird.

Deshalb prüfen:

```
Ist der Dienst wirklich nötig?
Ist der Dienst gepatcht?
Gibt es starke Authentifizierung?
Gibt es TLS?
```

Gibt es Logging?

Gibt es Firewall-Beschränkungen?

Gibt es eine DMZ?

Gibt es Alternativen wie VPN?

Merksatz:

Portweiterleitung nur gezielt und dokumentiert einsetzen.

DNS, DHCP, Gateway und NAT zusammen

Ein normaler Client braucht oft:

IP-Adresse von DHCP

Subnetzmaske von DHCP

Gateway von DHCP

DNS-Server von DHCP

Gateway für andere Netze

NAT für Internetzugriff mit privater IPv4-Adresse

DNS für Namensauflösung

Merksatz:

Internetzugriff braucht meistens mehrere korrekt zusammenspielende Bausteine.

Beispiel: Client kommt nicht ins Internet

Prüfreihenfolge:

1. Hat der Client eine gültige IP-Adresse?

2. Passt die Subnetzmaske?

3. Ist das Gateway eingetragen?

4. Liegt das Gateway im gleichen Subnetz?

5. Ist das Gateway erreichbar?

6. Funktioniert Zugriff auf externe IP?

7. Funktioniert DNS?

8. Funktioniert NAT?

9. Blockiert eine Firewall?

Merksatz:

Erst IP und Gateway,
dann DNS,
dann NAT und Firewall.

Beispiel: Webseite per IP erreichbar, per Name nicht

Fehlerbild:

Zugriff auf 93.184.216.34 funktioniert.

Zugriff auf www.example.com funktioniert nicht.

Wahrscheinliche Ursache:

DNS

Prüfen:

DNS-Server eingetragen?
DNS-Server erreichbar?

DNS-Eintrag korrekt?
anderer DNS-Server testen?
DNS-Cache leeren?

Merksatz:

Wenn IP funktioniert,
ist die Grundverbindung nicht das Hauptproblem.

Beispiel: Client hat 169.254.x.x

Fehlerbild:

Client hat APIPA-Adresse.

Wahrscheinliche Ursache:

DHCP nicht erreichbar

Prüfen:

Kabel oder WLAN
VLAN
DHCP-Server
DHCP-Scope
DHCP-Relay
Firewall
Switchport

Merksatz:

APIPA heißt:
automatische Notadresse statt gültiger DHCP-Adresse.

Beispiel: lokal erreichbar, Internet nicht

Fehlerbild:

Client erreicht Server im eigenen Netz.

Internet funktioniert nicht.

Mögliche Ursachen:

Gateway fehlt
Gateway falsch
Routingfehler
NAT fehlt
Firewall blockiert
DNS bei Namenszugriff zusätzlich möglich

Merksatz:

Lokale Kommunikation beweist nicht,
dass Gateway und NAT funktionieren.

Beispiel: Portweiterleitung funktioniert nicht

Mögliche Ursachen:

falscher externer Port
falsche interne IP
falscher interner Port
Dienst läuft nicht
lokale Firewall blockiert
Router-Firewall blockiert
NAT-Regel fehlt
doppelte NAT-Umgebung
öffentlicher DNS zeigt falsch
Provider blockiert Port

Merksatz:

Bei Portweiterleitung immer externen Port,
internes Ziel,

```
Dienst
und Firewall prüfen.
```

Doppeltes NAT

Doppeltes NAT bedeutet:

```
Verkehr wird durch zwei NAT-Geräte übersetzt.
```

Beispiel:

```
Provider-Router

und dahinter

eigener Router
```

Problem:

```
Portweiterleitungen werden schwieriger,
weil beide Geräte korrekt konfiguriert sein müssen.
```

Merksatz:

```
Doppeltes NAT erschwert eingehende Verbindungen.
```

CGNAT

CGNAT steht für:

```
Carrier-Grade NAT
```

Dabei teilt der Provider öffentliche IPv4-Adressen auf mehrere Kunden auf.

Problem:

```
Eigene Portweiterleitungen von außen funktionieren oft nicht direkt,
weil der Kunde keine eigene öffentliche IPv4-Adresse hat.
```

Merksatz:

```
Bei CGNAT ist eingehender Zugriff von außen eingeschränkt.
```

DNS bei Portweiterleitung

Für externen Zugriff braucht man oft zusätzlich DNS.

Beispiel:

```
app.firma.de
```

zeigt auf:

```
öffentliche IP-Adresse
```

Dann leitet NAT/Firewall weiter auf:

```
internen Server
```

Mögliche Fehler:

```
DNS zeigt auf falsche öffentliche IP
alter DNS-Cache
falscher A-Record
Split-DNS-Konflikt
```

Merksatz:

```
DNS findet die öffentliche Adresse,
NAT leitet zum internen Dienst.
```

NAT und Firewall unterscheiden

Begriff	Aufgabe
NAT	Adressen übersetzen
Firewall	Verkehr erlauben oder blockieren

Wichtig:

> In vielen Geräten sind NAT und Firewall kombiniert.
> Fachlich bleiben es unterschiedliche Funktionen.

Merksatz:

> NAT übersetzt.
> Firewall filtert.

DNS und DHCP unterscheiden

Begriff	Aufgabe
DNS	Namen auflösen
DHCP	IP-Konfiguration verteilen

Prüfungsfalle:

> Ein Client mit 169.254.x.x hat zuerst ein DHCP-Problem,
> nicht direkt ein DNS-Problem.

Merksatz:

> DHCP gibt die Konfiguration.
> DNS nutzt danach diese Konfiguration.

Gateway und NAT unterscheiden

Begriff	Aufgabe
Gateway	Router in andere Netze
NAT	Übersetzung von Adressen

Prüfungsfalle:

Ein Gateway kann vorhanden sein,
aber NAT kann trotzdem fehlen oder falsch sein.

Merksatz:

Gateway leitet weiter.
NAT übersetzt.

Typische Prüfungsfallen

DNS und DHCP verwechseln.

Gateway und DNS verwechseln.

NAT als Firewall bezeichnen.

PAT nicht als Port Address Translation erkennen.

Portweiterleitung mit normalem ausgehendem NAT verwechseln.

Gateway außerhalb des Client-Subnetzes eintragen.

DHCP-Relay vergessen.

APIPA nicht erkennen.

DNS nur mit UDP 53 verbinden und TCP 53 vergessen.

Private IPv4-Adressen als öffentlich routbar ansehen.

CGNAT bei eingehenden Verbindungen ignorieren.

Merksatz:

Die meisten Fehler entstehen durch Verwechslung der Aufgaben.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was macht DNS?
- Was macht DHCP?
- Was bedeutet DORA?
- Welche Ports nutzt DHCP?
- Welche Ports nutzt DNS?
- Was bedeutet eine Adresse aus 169.254.0.0/16?
- Was ist ein DHCP-Scope?
- Was ist eine DHCP-Reservierung?
- Was ist ein DHCP-Relay?
- Was ist ein Standardgateway?
- Warum muss das Gateway im lokalen Subnetz erreichbar sein?
- Was ist NAT?
- Was ist PAT?
- Was ist eine Portweiterleitung?
- Warum ersetzt NAT keine Firewall?
- Warum funktioniert Zugriff per IP, aber nicht per Name?

IHK-sichere Kurzformulierung

DNS, DHCP, Gateway und NAT erfüllen unterschiedliche Aufgaben im Netzwerk. DNS löst Namen in IP-Adressen auf. DHCP verteilt automatisch Netzwerkkonfigurationen wie IP-Adresse, Subnetzmaske, Gateway und DNS-Server. Das Standardgateway ist der Router, über den ein Client andere Netze erreicht. NAT übersetzt IP-Adressen, häufig private interne IPv4-Adressen in eine öffentliche Adresse. PAT nutzt zusätzlich Ports, damit mehrere interne Clients über eine öffentliche IP-Adresse kommunizieren können. Portweiterleitung macht interne Dienste von außen erreichbar und erhöht dadurch die Angriffsfläche. Typische Fehlerbilder sind: IP funktioniert, Name nicht = DNS; 169.254.x.x = DHCP; lokal funktioniert, Internet nicht = Gateway, Routing, NAT oder Firewall.

Merksätze

DNS löst Namen auf.

DHCP verteilt IP-Konfiguration.

Gateway führt in andere Netze.

NAT übersetzt Adressen.

PAT nutzt Ports.

Portweiterleitung veröffentlicht Dienste.

DNS nutzt UDP und TCP 53.

DHCP nutzt UDP 67 und 68.

DHCP-DORA:
Discover,
Offer,
Request,
Acknowledge.

169.254.x.x deutet auf DHCP-Problem.

DHCP-Scope ist der Adresspool.

DHCP-Lease ist zeitlich begrenzte Vergabe.

DHCP-Reservierung gibt einem Gerät immer dieselbe IP.

DHCP-Relay leitet DHCP-Anfragen in andere Netze.

Gateway muss im lokalen Subnetz erreichbar sein.

Standardroute ist 0.0.0.0/0.

Spezifischste Route gewinnt.

Private IPv4-Adressen werden im Internet nicht direkt geroutet.

NAT ersetzt keine Firewall.

NAT übersetzt,
Firewall filtert.

DNS findet die öffentliche Adresse,
NAT leitet nach intern weiter.

Doppeltes NAT erschwert Portweiterleitungen.

CGNAT erschwert eingehende Verbindungen.

IP ja,
Name nein:
DNS.

169.254.x.x:
DHCP.

Lokal ja,
extern nein:
Gateway,
Routing,
NAT,
Firewall.

Host ja,
Dienst nein:
Port,
Dienst,
Firewall.